U.S. Serial No. 09/783,112

REMARKS

Claims 1, 10, and 26-28 are pending.
Claims 1, 10 and 26-28 are rejected.

The office action dated October 5, 2005 indicates that claims 1, 10 and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chuang U.S. Patent No. 6,003,151 in view of Kangas U.S. Patent No. 5,355,412. This rejection is respectfully traversed.

The claimed inventions offer solutions to the following problem: how to send ECC blocks to a computer over an insecure bus without (1) destroying the integrity of the ECC code words; and (2) not leaving the ECC blocks vulnerable to theft and unauthorized copying. The documents made of record, alone and in the aggregate, do not teach or suggest a solution to this problem.

Chuang is not relevant to this problem. Chuang is concerned with increasing the throughput from an optical drive to a computer data bus (col. 3, lines 43-45). Chuang purportedly increases the throughput by modifying error detection and correction.

Chuang does not teach or suggest that ECC coding is performed outside of the optical drive. Chuang clearly discloses that ECC coding is necessarily performed within the optical drive. See col. 1, lines 60+ (a variety of operations "must be" performed on data read from a CD disk before the data can be provided to the data buses of a host computer, including error correction).

The office action cites a passage at col. 4, lines 45-50, and alleges that Chuang's error correction is performed by a host processor. Taken in a vacuum, the passage is vague at best. It is not clear whether error correction

is performed within the optical CD drive.

However, when this passage is read in conjunction with the remainder of Chuang's specification, it is quite clear that data is read from an optical disk, and error correction is performed in an optical drive. See Figure 3, which illustrates Chuang's optical disk mass storage system (col. 4, lines 26-28). A controller 58 performs error correction on ECC blocks before the corrected user data is sent to an IDE bus 64 (col.7, lines 13-14).

Chuang does not teach or suggest a bitwise XOR of an encryption mask and a block of ECC-encoded data. Chuang describes XOR operations in connection with error check division (col. 3, lines 19-30), which is part of error detection.

Chuang does not even teach or suggest encrypting ECC blocks . If the examiner insists otherwise, he is respectfully respected to pinpoint cite and quote the exact words that describe encryption.

Kangas does not teach or suggest the differences between the claims and Chuang. Kangas discloses a checksum for a secret message. The checksum is used to determine whether a secret message was transmitted successfully. Kangas's checksum also identifies the party for whom the message is intended (col. 2, line 15).

Kangas does not teach or suggest that his "secret message" is an ECC block. Therefore, Kangas does not teach or suggest encryption of ECC blocks, let alone XOR encryption.

Kangas only discloses XOR operations of different checksums. The checksum of the secret message is XOR'ed with the CRC-identifier of each "receiving" person (col. 3, lines 15-18). **Kangas does not teach or suggest a**

bitwise XOR of an encryption mask and a block of ECC-encoded data.

Kangas does not teach or suggest that XOR encryption will preserve the integrity of ECC code words.

Kangas does not even teach or suggest error correction. Kangas's checksum only indicates whether the secret message was transmitted with errors.

Kangas isn't even analogous art within the meaning of MPEP 2141.01(a). "In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned. Kangas relates to a the transmission of multi-point network unique messages to different parties (col. 1, lines 13-15), and he is concerned with "identifying to whom a message is potentially transmitted without increasing the number of bits in the information transmitted and without needing to open all the secret data messages" (col. 1, lines 39-43).

The office action alleges that XOR operations on ECC blocks are disclosed at col. 2, lines 10-40 of Kangas; and that the host processor can perform error correction at col. 3, line 50 to col. 4, line 20 of Kangas. There is no support for these allegations. If the examiner insists otherwise, he is respectfully respected to pinpoint cite and quote the exact words that support his allegations. If he alleges that the secret message and checksum constitute an ECC block, he is respectfully requested to find support in the prior art for the allegation, or submit an affidavit pursuant to MPEP §707 and 37 CFR §1.104(d)(2).

The office action also gives a reason for modifying Chuang in

accordance with Kangas. The reason is allegedly found in a passage at col. 1, lines 30-35. However, the reason is irrelevant with respect to Chuang, since Chuang does not teach or suggest that the data on the IDE bus is intended for different receiving parties.

The cited documents, alone and in combination, do not teach or suggest a solution to the problem addressed by the applicant, nor do they teach or suggest the system of claim 26, the drive of claim 27, or the controller of claim 28. For these reasons, the '103 rejections of claims 1, 10, and 26-28 should be withdrawn.

Although point is moot, the office action indicates that the allowability of claims 1, 10 and 26 was withdrawn in view of Chuang and Kangas. However, the previous office action indicated that only claim 10 contained allowable subject matter.

Claims 1 and 26 are rejected in view of claim 8 in U.S. Patent No. 6,252,961 under the judicially-created doctrine of double-patenting. This rejection is respectfully traversed. Consider the following differences between claim 8 of the '961 patent and claim 26 of the present application:

1. The drive of claim 8 includes means for providing a block of ECC-encoded data. The drive of claim 26 does not recite this feature.

2. In the drive of claim 8, an output of the bitwise XOR means is coupled to a computer bus. Claim 26 recites a drive that provides an encrypted block to a computer bus.

3. In the drive of claim 8, the encryption mask is coded according to the same error code correction method. The drive of claim 26 does not recite this feature.

It is up to the examiner to show that these differences would be obvious to a person skilled in the art. The examiner has yet to make such a showing. See MPEP 804 (II)(B)(1). The office action does not provide evidence in the prior art of the level of skill. The examiner simply relies on the '961 patent and provides a personal opinion of obviousness. However, the '961 patent is not prior art, and an examiner's personal opinion does not constitute evidence.

Claim 1 is objected to as being a substantial duplicate of claim 26. However, this issue was rendered moot by the response filed Jan. 15, 2005, in which claim 1 was amended to depend from claim 26. Claim 26 recites a drive, but does not recite structure for the drive. Claim 1 recites the structure of the drive in terms of means-plus-function language. If the examiner maintains this objection, he is respectfully requested to provide an explanation.

It is respectfully submitted that the present application is in condition for allowance. The examiner is encouraged to contact applicant's attorney Hugh Gortler to discuss any issues that might remain.